United States Government Accountability Office

GAO

Testimony

Before the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, Committee on Homeland Security, House of Representatives

For Release on Delivery
Expected at 2:00 p.m. DST
Tuesday, March 10, 2009

NATIONAL CYBERSECURITY STRATEGY

Key Improvements Are Needed to Strengthen the Nation's Posture

Statement of David Powner,
Director, Information Technology Management Issues

Report Documentation Page

Form Approved
OMB No. 0704-0188

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
10 MAR 2009		**00-00-2009 to 00-00-2009**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
National Cybersecurity Strategy: Key Improvements Are Needed to Strengthen the Nation's Posture	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **Government Accountability Office,Testimony Before the Subcommittee on Emerging Threats,,Cybersecurity, and Science and Technology,Washington,DC**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release; distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT **unclassified**	b. ABSTRACT **unclassified**	c. THIS PAGE **unclassified**	**Same as Report (SAR)**	**18**	

March 10, 2009

NATIONAL CYBERSECURITY STRATEGY

Key Improvements Are Needed to Strengthen the Nation's Posture

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-09-432T, a testimony to the Subcommittee on Emerging Threats, Cybersecurity, and Science and Technology, Committee on Homeland Security, House of Representatives

Why GAO Did This Study

Pervasive and sustained computer-based (cyber) attacks against federal and private-sector infrastructures pose a potentially devastating impact to systems and operations and the critical infrastructures that they support. To address these threats, President Bush issued a 2003 national strategy and related policy directives aimed at improving cybersecurity nationwide. Congress and the Executive Branch, including the new administration, have subsequently taken actions to examine the adequacy of the strategy and identify areas for improvement. Nevertheless, GAO has identified this area as high risk and has reported on needed improvements in implementing the national cybersecurity strategy.

In this testimony, you asked GAO to summarize (1) key reports and recommendations on the national cybersecurity strategy and (2) the views of experts on how to strengthen the strategy. In doing so, GAO relied on its previous reports related to the strategy and conducted panel discussions with key cybersecurity experts to solicit their views on areas for improvement.

What GAO Recommends

GAO has previously made about 30 recommendations, mostly directed at DHS, to improve our nation's cybersecurity strategy efforts. DHS in large part has concurred with GAO's recommendations and, in many cases, has actions planned and under way to implement them.

View GAO-09-432T or key components. For more information, contact David A. Powner at (202) 512-9286 or pownerd@gao.gov.

What GAO Found

Over the last several years, GAO has consistently reported that the Department of Homeland Security (DHS) has yet to fully satisfy its responsibilities designated by the national cybersecurity strategy. To address these shortfalls, GAO has made about 30 recommendations in key cybersecurity areas including the 5 listed in the table below. While DHS has since developed and implemented certain capabilities to satisfy aspects of its cybersecurity responsibilities, it still has not fully satisfied the recommendations, and thus further action needs to be taken to fully address these areas.

Key Cybersecurity Areas Identified by GAO as Needing Further Action
1. Bolstering cyber analysis and warning capabilities
2. Completing actions identified during cyber exercises
3. Improving cybersecurity of infrastructure control systems
4. Strengthening DHS's ability to help recover from Internet disruptions
5. Addressing cybercrime

Source: GAO analysis of prior GAO reports.

In discussing the areas addressed by GAO's recommendations as well as other critical aspects of the strategy, GAO's panel of cybersecurity experts identified 12 key areas requiring improvement (see table below). GAO found these to be largely consistent with its reports and its extensive research and experience in the area.

Key Strategy Improvements Identified by Cybersecurity Experts	
1.	Develop a national strategy that clearly articulates strategic objectives, goals, and priorities.
2.	Establish White House responsibility and accountability for leading and overseeing national cybersecurity policy.
3.	Establish a governance structure for strategy implementation.
4.	Publicize and raise awareness about the seriousness of the cybersecurity problem.
5.	Create an accountable, operational cybersecurity organization.
6.	Focus more actions on prioritizing assets, assessing vulnerabilities, and reducing vulnerabilities than on developing additional plans.
7.	Bolster public/private partnerships through an improved value proposition and use of incentives.
8.	Focus greater attention on addressing the global aspects of cyberspace.
9.	Improve law enforcement efforts to address malicious activities in cyberspace.
10.	Place greater emphasis on cybersecurity research and development, including consideration of how to better coordinate government and private sector efforts.
11.	Increase the cadre of cybersecurity professionals.
12.	Make the federal government a model for cybersecurity, including using its acquisition function to enhance cybersecurity aspects of products and services.

Source: GAO analysis of opinions solicited during expert panels.

Until GAO's recommendations are fully addressed and the above improvements are considered, our nation's federal and private-sector infrastructure systems remain at risk of not being adequately protected. Consequently, in addition to fully implementing GAO's recommendations, it is essential that the improvements be considered by the new administration as it begins to make decisions on our nation's cybersecurity strategy.

Madam Chair and Members of the Subcommittee:

Thank you for the opportunity to join in today's hearing to discuss efforts to protect our nation from cybersecurity threats. Pervasive and sustained computer-based (cyber) attacks against the United States and others continue to pose a potentially devastating impact to systems and operations and the critical infrastructures that they support. To address these threats, President Bush issued a 2003 national strategy and related policy directives aimed at improving cybersecurity nationwide, including both government systems and those cyber critical infrastructures owned and operated by the private sector.[1]

Because the threats have persisted and grown, a commission—commonly referred to as the Commission on Cybersecurity for the 44th Presidency and chaired by two congressmen and industry officials—was established in August 2007 to examine the adequacy of the strategy and identify areas for improvement.[2] At about the same time, the Bush Administration began to implement a series of initiatives aimed primarily at improving cybersecurity within the federal government. More recently, in February 2009, President Obama initiated a review of the government's overall cybersecurity strategy and supporting activities.

Today, as requested, I will discuss (1) our reports, containing about 30 recommendations, on the national cybersecurity strategy and

[1] Critical infrastructures are systems and assets, whether physical or virtual, so vital to nations that their incapacity or destruction would have a debilitating impact on national security, national economic security, national public health or safety, or any combination of those matters. Federal policy established 18 critical infrastructure sectors: agriculture and food, banking and finance, chemical, commercial facilities, communications, critical manufacturing, dams, defense industrial base, emergency services, energy, government facilities, information technology, national monuments and icons, nuclear reactors, materials and waste, postal and shipping, public health and health care, transportation systems, and water.

[2] The commission was created by the Center for Strategic and International Studies (CSIS), a bipartisan, nonprofit organization that, among other things, provides strategic insights and policy solutions to decision makers. Entitled the CSIS Commission on Cybersecurity for the 44th Presidency, the body was co-chaired by Representative James Langevin, Representative Michael McCaul, Scott Charney (Microsoft), and Lt. General Harry Raduege, USAF (Ret).

related efforts and (2) the results of expert panels we convened to discuss how to strengthen the strategy and our nation's cybersecurity posture. In preparing for this testimony, we relied on our previous reports on federal efforts to fulfill national cybersecurity responsibilities. These reports contain detailed overviews of the scope and methodology we used. We also obtained the views of nationally recognized cybersecurity experts by means of two panel discussions on the effectiveness of the current national cybersecurity strategy and recommendations for improvement. In summarizing the panel discussions, we provided all panel members an opportunity to comment on our written summaries, and their comments were incorporated as appropriate. The panelists' names and titles are in appendix I. We conducted our work in support of this testimony during February and March 2009, in the Washington, D.C., area. The work on which this testimony is based was performed in accordance with generally accepted government auditing standards.

Background

Government officials are concerned about attacks from individuals and groups with malicious intent, such as criminals, terrorists, and adversarial foreign nations. For example, in February 2009, the Director of National Intelligence testified that foreign nations and criminals have targeted government and private sector networks to gain a competitive advantage and potentially disrupt or destroy them, and that terrorist groups have expressed a desire to use cyber attacks as a means to target the United States.[3] The director also discussed that in August 2008, the national government of Georgia's Web sites were disabled during hostilities with Russia, which hindered the government's ability to communicate its perspective about the conflict.

[3] Statement of the Director of National Intelligence before the Senate Select Committee on Intelligence, *Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence* (Feb. 12, 2009).

The federal government has developed a strategy to address such cyber threats. Specifically, President Bush issued the 2003 *National Strategy to Secure Cyberspace*[4] and related policy directives, such as Homeland Security Presidential Directive 7,[5] that specify key elements of how the nation is to secure key computer-based systems, including both government systems and those that support critical infrastructures owned and operated by the private sector. The strategy and related policies also establish the Department of Homeland Security (DHS) as the focal point for cyber CIP and assign the department multiple leadership roles and responsibilities in this area. They include (1) developing a comprehensive national plan for CIP, including cybersecurity; (2) developing and enhancing national cyber analysis and warning capabilities; (3) providing and coordinating incident response and recovery planning, including conducting incident response exercises; (4) identifying, assessing, and supporting efforts to reduce cyber threats and vulnerabilities, including those associated with infrastructure control systems;[6] and (5) strengthening international cyberspace security. In addition, the strategy and related policy direct DHS and other relevant stakeholders to use risk management principles to prioritize protection activities within and across the 18 critical infrastructure sectors in an integrated, coordinated fashion.

Because the threats have persisted and grown, President Bush in January 2008 began to implement a series of initiatives—commonly referred to as the Comprehensive National Cybersecurity Initiative (CNCI)—aimed primarily at improving DHS and other federal agencies' efforts to protect against intrusion attempts and anticipate future threats.[7] While these initiatives have not been made public,

[4] The White House, *The National Strategy to Secure Cyberspace* (Washington, D.C.: February 2003).

[5] The White House, Homeland Security Presidential Directive 7 (Washington, D.C.: Dec. 17, 2003).

[6] Control systems are computer-based systems that perform vital functions in many of our nation's critical infrastructures, including electric power generation, transmission, and distribution; oil and gas refining and pipelines; water treatment and distribution; chemical production and processing; railroads and mass transit; and manufacturing.

[7] The White House, National Security Presidential Directive 54/Homeland Security Presidential Directive 23 (Washington, D.C.: Jan. 8, 2008).

the Director of National Intelligence stated that they include defensive, offensive, research and development, and counterintelligence efforts, as well as a project to improve public/private partnerships.[8] Subsequently, in December 2008, the Commission on Cybersecurity for the 44th Presidency reported, among other things, that the failure to protect cyberspace was an urgent national security problem and made 25 recommendations aimed at addressing shortfalls with the strategy and its implementation.[9] Since then, President Obama (in February 2009) initiated a review of the cybersecurity strategy and supporting activities. The review is scheduled to be completed in April 2009.

GAO Has Made Recommendations to Address Shortfalls with Key Aspects of National Cybersecurity Strategy and its Implementation

Over the last several years we have reported on our nation's efforts to fulfill essential aspects of its cybersecurity strategy. In particular, we have reported consistently since 2005 that DHS has yet to fully satisfy its cybersecurity responsibilities designated by the strategy. To address these shortfalls, we have made about 30 recommendations in key cybersecurity areas including the 5 listed in table 1. DHS has since developed and implemented certain capabilities to satisfy aspects of its cybersecurity responsibilities, but the department still has not fully satisfied our recommendations, and thus further action needs to be taken to address these areas.

[8] Statement of the Director of National Intelligence before the Senate Select Committee on Intelligence, *Annual Threat Assessment of the Intelligence Community for the Senate Select Committee on Intelligence* (Feb. 12, 2009).

[9] Center for Strategic and International Studies, *Securing Cyberspace for the 44th Presidency*, *A Report of the CSIS Commission on Cybersecurity for the 44th Presidency* (Washington, D.C.: December 2008).

Table 1: Key Cybersecurity Areas Identified by GAO As Needing Further Action

1. Bolstering cyber analysis and warning capabilities
2. Completing actions identified during cyber exercises
3. Improving cybersecurity of infrastructure control systems
4. Strengthening DHS's ability to help recover from Internet disruptions
5. Addressing cybercrime

Source: GAO analysis of prior GAO reports.

In July 2008, we reported[10] that DHS's United States Computer Emergency Readiness Team (US-CERT) did not fully address 15 key cyber analysis and warning attributes related to (1) monitoring network activity to detect anomalies, (2) analyzing information and investigating anomalies to determine whether they are threats, (3) warning appropriate officials with timely and actionable threat and mitigation information, and (4) responding to the threat. For example, US-CERT provided warnings by developing and distributing a wide array of notifications; however, these notifications were not consistently actionable or timely. As a result, we recommended that the department address shortfalls associated with the 15 attributes in order to fully establish a national cyber analysis and warning capability as envisioned in the national strategy. DHS agreed in large part with our recommendations.

In September 2008, we reported[11] that since conducting a major cyber attack exercise, called Cyber Storm, DHS had demonstrated progress in addressing eight lessons it had learned from these efforts. However, its actions to address the lessons had not been fully implemented. Specifically, while it had completed 42 of the 66 activities identified, the department had identified 16 activities as ongoing and 7 as planned for the future.[12] Consequently, we recommended that DHS schedule and complete all of the corrective activities identified in order to strengthen coordination between

[10] GAO, *Cyber Analysis and Warning: DHS Faces Challenges in Establishing a Comprehensive National Capability*, GAO-08-588 (Washington, D.C.: July 31, 2008).

[11] GAO, *Critical Infrastructure Protection: DHS Needs To Fully Address Lessons Learned from Its First Cyber Storm Exercise*, GAO-08-825 (Washington, D.C.: Sept. 9, 2008).

[12] At that time, DHS reported that one other activity had been completed, but the department was unable to provide evidence demonstrating its completion.

public and private sector participants in response to significant cyber incidents. DHS concurred with our recommendation. To date, DHS has continued to make progress in completing some identified activities but has yet to do so for others.

In a September 2007 report and an October 2007 testimony, we reported[13] that consistent with the national strategy requirement to identify and reduce threats and vulnerabilities, DHS was sponsoring multiple control systems security initiatives, including an effort to improve control systems cybersecurity using vulnerability evaluation and response tools. However, DHS had not established a strategy to coordinate the various control systems activities across federal agencies and the private sector, and it did not effectively share information on control system vulnerabilities with the public and private sectors. Accordingly, we recommended that DHS develop a strategy to guide efforts for securing control systems and establish a rapid and secure process for sharing sensitive control system vulnerability information. DHS recently began developing a strategy and a process to share sensitive information.

We reported and later testified[14] in 2006 that the department had begun a variety of initiatives to fulfill its responsibility, as called for by the national strategy, for developing an integrated public/private plan for Internet recovery. However, we determined that these efforts were not comprehensive or complete. As such, we recommended that DHS implement nine actions to improve the department's ability to facilitate public/private efforts to recover the Internet in case of a major disruption. In October 2007, we testified[15] that the department had made progress in implementing our

[13] GAO, *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain*, GAO-07-1036 (Washington, D.C.: Sept. 10, 2007) and *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain*, GAO-08-119T (Washington, D.C.: Oct. 17, 2007).

[14] GAO, *Internet Infrastructure: DHS Faces Challenges in Developing a Joint Public/Private Recovery Plan*, GAO-06-672 (Washington, D.C.: June 16, 2006) and *Internet Infrastructure: Challenges in Developing a Public/Private Recovery* Plan, GAO-06-863T (Washington, D.C.: July 28, 2006).

[15] GAO, *Internet Infrastructure: Challenges in Developing a Public/Private Recovery Plan*, GAO-08-212T (Washington, D.C.: Oct. 23, 2007).

recommendations; however, seven of the nine have not been completed. To date, an integrated public/private plan for Internet recovery does not exist.

In 2007, we reported[16] that public and private entities[17] faced a number of challenges in addressing cybercrime, including ensuring adequate analytical and technical capabilities for law enforcement and conducting investigations and prosecuting cybercrimes that cross national and state borders.

Cybersecurity Experts Highlighted Key Improvements Needed to Strengthen the Nation's Cybersecurity Posture

In addition to our recommendations on improving key aspects of the national cybersecurity strategy and its implementation, we also obtained the views of experts (by means of panel discussions) on these and other critical aspects of the strategy, including areas for improvement. The experts, who included former federal officials, academics, and private sector executives, highlighted 12 key improvements that are, in their view, essential to improving the strategy and our national cybersecurity posture. These improvements are in large part consistent with our above mentioned reports and extensive research and experience in this area. They include:

1. **Develop a national strategy that clearly articulates strategic objectives, goals, and priorities**—The strategy should, among other things, (1) include well-defined strategic objectives, (2) provide understandable goals for the government and the private sector (end game), (3) articulate cyber priorities among the objectives, (4) provide a vision of what secure cyberspace should be in the future, (5) seek to integrate federal

[16] GAO, *Cybercrime: Public and Private Entities Face Challenges in Addressing Cyber Threats*, GAO-07-705 (Washington, D.C.: June 2007).

[17] These public and private entities include the Departments of Justice, Homeland Security, and Defense, and the Federal Trade Commission, Internet security providers and software developers.

government capabilities, (6) establish metrics to gauge whether progress is being made against the strategy, and (7) provide an effective means for enforcing action and accountability when there are progress shortfalls. According to expert panel members, the CNCI provides a good set of tactical initiatives focused on improving primarily federal cybersecurity; however, it does not provide strategic objectives, goals, and priorities for the nation as a whole.

2. **Establish White House responsibility and accountability for leading and overseeing national cybersecurity policy**—The strategy makes DHS the focal point for cybersecurity; however, according to expert panel members, DHS has not met expectations and has not provided the high-level leadership needed to raise cybersecurity to a national focus. Accordingly, panelists stated that to be successful and to send the message to the nation and cyber critical infrastructure owners that cybersecurity is a priority, this leadership role needs to be elevated to the White House. In addition, to be effective, the office must have, among other things, commensurate authority—for example, over budgets and resources—to implement and employ appropriate incentives to encourage action.

3. **Establish a governance structure for strategy implementation**—The strategy establishes a public/private partnership governance structure that includes 18 critical infrastructure sectors, corresponding government and sector coordinating councils, and cross-sector councils. However, according to panelists, this structure is government-centric and largely relies on personal relationships to instill trust to share information and take action. In addition, although all sectors are not of equal importance in regard to their cyber assets and functions, the structure treats all sectors and all critical cyber assets and functions equally. To ensure effective strategy implementation, experts stated that the partnership structure should include a committee of senior government representatives (for example, the Departments of Defense, Homeland Security, Justice, State, and the Treasury and the White House) and private sector leaders representing the most critical cyber assets and functions. Expert panel members also

suggested that this committee's responsibilities should include measuring and periodically reporting on progress in achieving the goals, objectives, and strategic priorities established in the national strategy and building consensus to hold involved parties accountable when there are progress shortfalls.

4. **Publicize and raise awareness about the seriousness of the cybersecurity problem**—Although the strategy establishes cyberspace security awareness as a priority, experts stated that many national leaders in business and government, including in Congress, who can invest resources to address cybersecurity problems are generally not aware of the severity of the risks to national and economic security posed by the inadequacy of our nation's cybersecurity posture and the associated intrusions made more likely by that posture. Expert panel members suggested that an aggressive awareness campaign is needed to raise the level of knowledge of leaders and the general populace that our nation is constantly under cyber attack.

5. **Create an accountable, operational cybersecurity organization**—DHS established the National Cyber Security Division (within the Office of Cybersecurity and Communications) to be responsible for leading national day-to-day cybersecurity efforts; however, according to panelists, this has not enabled DHS to become the national focal point as envisioned. Panel members stated that currently, DOD and other organizations within the intelligence community that have significant resources and capabilities have come to dominate federal efforts. They told us that there also needs to be an independent cybersecurity organization that leverages and integrates the capabilities of the private sector, civilian government, law enforcement, military, intelligence community, and the nation's international allies to address incidents against the nation's critical cyber systems and functions. However, there was not consensus among our expert panel members regarding where this organization should reside.

6. **Focus more actions on prioritizing assets and functions, assessing vulnerabilities, and reducing vulnerabilities than on developing additional plans**—The strategy recommends

actions to identify critical cyber assets and functions, but panelists stated that efforts to identify which cyber assets and functions are most critical to the nation have been insufficient. According to panel members, inclusion in cyber critical infrastructure protection efforts and lists of critical assets are currently based on the willingness of the person or entity responsible for the asset or function to participate and not on substantiated technical evidence. In addition, the current strategy establishes vulnerability reduction as a key priority; however, according to panelists, efforts to identify and mitigate known vulnerabilities have been insufficient. They stated that greater efforts should be taken to identify and eliminate common vulnerabilities and that there are techniques available that should be used to assess vulnerabilities in the most critical, prioritized cyber assets and functions.

7. **Bolster public/private partnerships through an improved value proposition and use of incentives**—While the strategy encourages action by owners and operators of critical cyber assets and functions, panel members stated that there are not adequate economic and other incentives (i.e., a value proposition) for greater investment and partnering in cybersecurity. Accordingly, panelists stated that the federal government should provide valued services (such as offering useful threat or analysis and warning information) or incentives (such as grants or tax reductions) to encourage action by and effective partnerships with the private sector. They also suggested that public and private sector entities use means such as cost-benefit analyses to ensure the efficient use of limited cybersecurity-related resources.

8. **Focus greater attention on addressing the global aspects of cyberspace**—The strategy includes recommendations to address the international aspects of cyberspace but, according to panelists, the U.S. is not addressing global issues impacting how cyberspace is governed and controlled. They added that, while other nations are actively involved in developing treaties, establishing standards, and pursuing international agreements (such as on privacy), the U.S. is not aggressively working in a coordinated manner to ensure that international agreements are

consistent with U.S. practice and that they address cybersecurity and cybercrime considerations. Panel members stated that the U.S. should pursue a more coordinated, aggressive approach so that there is a level playing field globally for U.S. corporations and enhanced cooperation among government agencies, including law enforcement. In addition, a panelist stated that the U.S. should work towards building consensus on a global cyber strategy.

9. **Improve law enforcement efforts to address malicious activities in cyberspace**—The strategy calls for improving investigative coordination domestically and internationally and promoting a common agreement among nations on addressing cybercrime. According to a panelist, some improvements in domestic law have been made (e.g., enactment of the PROTECT Our Children Act of 2008), but implementation of this act is a work in process due to its recent passage. Panel members also stated that current domestic and international law enforcement efforts, including activities, procedures, methods, and laws are too outdated and outmoded to adequately address the speed, sophistication, and techniques of individuals and groups, such as criminals, terrorists, and adversarial foreign nations with malicious intent. An improved law enforcement is essential to more effectively catch and prosecute malicious individuals and groups and, with stricter penalties, deter malicious behavior.

10. **Place greater emphasis on cybersecurity research and development, including consideration of how to better coordinate government and private sector efforts—**While the strategy recommends actions to develop a research and development agenda and coordinate efforts between the government and private sectors, experts stated that the U.S. is not adequately focusing and funding research and development efforts to address cybersecurity or to develop the next generation of cyberspace to include effective security capabilities. In addition, the research and development efforts currently underway are not being well coordinated between government and the private sector.

11. **Increase the cadre of cybersecurity professionals—**The strategy includes efforts to increase the number and skills of cybersecurity professionals but, according to panelists, the results have not created sufficient numbers of professionals, including information security specialists and cybercrime investigators. Expert panel members stated that actions to increase the number of professionals with adequate cybersecurity skills should include (1) enhancing existing scholarship programs (e.g., Scholarship for Service) and (2) making the cybersecurity discipline a profession through testing and licensing.

12. **Make the federal government a model for cybersecurity, including using its acquisition function to enhance cybersecurity aspects of products and services**—The strategy establishes securing the government's cyberspace as a key priority and advocates using federal acquisition to accomplish this goal. Although the federal government has taken steps to improve the cybersecurity of agencies (e.g., beginning to implement the CNCI initiatives), panelists stated that it still is not a model for cybersecurity. Further, they said the federal government has not made changes in its acquisition function and the training of government officials in a manner that effectively improves the cybersecurity capabilities of products and services purchased and used by federal agencies.

- - - -

In summary, our nation is under cyber attack, and the present strategy and its implementation have not been fully effective in mitigating the threat. This is due in part to the fact that there are further actions needed by DHS to address key cybersecurity areas, including fully addressing our recommendations. In addition, nationally recognized experts have identified improvements aimed at strengthening the strategy and in turn, our cybersecurity posture. Key improvements include developing a national strategy that clearly articulates strategic objectives, goals, and priorities; establishing White House leadership; improving governance; and creating a capable and respected operational lead organization. Until the recommendations are fully addressed and these

improvements are considered, our nation's most critical federal and private sector infrastructure systems remain at unnecessary risk to attack from our adversaries. Consequently, in addition to fully implementing our recommendations, it is essential that the Obama administration consider these improvements as it reviews our nation's cybersecurity strategy and begins to make decisions on moving forward.

Madam Chair, this concludes my statement. I would be happy to answer any questions that you or members of the subcommittee may have at this time.

If you have any questions on matters discussed in this testimony, please contact me at (202) 512-9286, or by e-mail at pownerd@gao.gov. Other key contributors to this testimony include Bradley Becker, Camille Chaires, Michael Gilmore, Nancy Glover, Kush Malhotra, Gary Mountjoy, Lee McCracken, and Andrew Stavisky.

Appendix I: Cybersecurity Expert Panel Participants

Steve D. Crocker, Chair, Security and Stability Advisory Committee, Internet Corporation for Assigned Names and Numbers.

Robert Dix, Vice President of Government Affairs, Juniper Networks, Inc.

Martha Stansell-Gamm, (Retired) Chief, Computer Crime and Intellectual Property Section, Department of Justice.

Dr. Lawrence Gordon, Ernst & Young Alumni Professor of Managerial Accounting and Information Assurance, Robert H. Smith School of Business, University of Maryland.

Tiffany Jones, Director, Public Policy and Government Relations, Symantec.

Tom Kellerman, Vice President of Security Awareness, Core Security.

Dr. Kathleen Kiernan, Chief Executive Officer, The Kiernan Group, and Chairman of the Board, InfraGard.

Cheri McGuire, Principal Security Strategist, Microsoft Corporation, and former Acting Director, National Cyber Security Division, U.S. Department of Homeland Security.

Allan Paller, Director of Research, SANS Institute.

Andy Purdy, President, DRA Enterprises, Inc., and former Acting Director, National Cyber Security Division, U.S. Department of Homeland Security.

Marcus Sachs, Executive Director of Government Affairs for National Security Policy, Verizon Communications; and Director, SANS Internet Storm Center.

Howard Schmidt, President and Chief Executive Officer, Information Security Forum.

David Sobel, Senior Counsel, Electronic Frontier Foundation.

Amit Yoran, Chairman and Chief Executive Officer, NetWitness Corporation; former Director, National Cyber Security Division, U.S. Department of Homeland Security.